UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,432	02/17/2004	Teddy C. Johnson	200312996-1	1557

22879 7590 08/10/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
BELANI, KISHIN G	

ART UNIT	PAPER NUMBER
2143	

MAIL DATE	DELIVERY MODE
08/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/780,432	JOHNSON, TEDDY C.	
	Examiner	Art Unit	
	Kishin G. Belani	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All. b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 1-3, 17-21, 30 and 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Freund (U.S. Patent Publication # 5,987,611)** in view of **Peled et al. (U.S. Patent Application Publication # 2002/0129140 A1).**

Consider **claim 1**, Freund shows and discloses a system for monitoring data transferred via an FTP protocol (Fig. 3A, system 300; column 14, lines 52-67 and column 15, lines 1-11 that disclose the details of the system shown in Fig. 3A; column

16, lines 25-29 that disclose monitoring of files transferred via FTP protocol);

comprising:

a client (Fig. 3A, Client blocks 310a-c; column 14, lines 54-59 that describe these clients);

a server operating as an intermediary between said client and a foreign network (Fig. 3A, server block 321, the Internet block 340 and foreign network block 350; column 14, lines 62-67 that describe the server in more details; column 15, lines 5-11 that disclose remote servers connected to the Internet);

an audit database (Fig. 5, audit log 580 used as an audit database; column 21, lines 41-46 that disclose the same details); and

an audit module (although Freund does not explicitly show a separate audit module, its functionality is incorporated within the data interpretation module 560 (shown in Fig. 5) that is part of the supervisory module 323 shown in Fig. 3A and disclosed in column 21, lines 41-46).

However, Freund does not explicitly show and disclose an audit module comprising logic for monitoring said data transferred via FTP protocol; and

logic for recording at least a portion of said data transferred via FTP protocol to said audit database.

In the same field of endeavor, Peled et al. do show and disclose an audit module comprising logic for monitoring said data transferred via FTP protocol (Fig. 1, Report Generator block 109 (same block listed as Audit Generator 409 in Fig. 4) along with the blocks 103, 105, and 106 that collectively provide logic for monitoring file transfer via

FTP protocol; Fig. 9, FTP proxy block 980 with FTP Monitor 9801; paragraph 216, lines 5-10 that disclose an FTP proxy 980 in use); and

logic for recording at least a portion of said data transferred via FTP protocol to said audit database (Fig. 7, Audit Generator block 709; paragraph 0170, lines 13-21 that disclose recording relevant details of the transferred content stored in an audit database 110 shown in Fig. 1).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include an audit module comprising logic for monitoring said data transferred via FTP protocol; with logic for recording at least a portion of said data transferred via FTP protocol to said audit database, as taught by Peled et al., in the system of Freund, so as to provide documented evidence of an employee's misuse of the company's IT resources.

Consider **claim 2**, and **as it applies to claim 1 above**, Freund further discloses a system for the claimed invention, wherein said client is capable of receiving data from said foreign network (column 4, line 67 and column 5, lines 1-5 which disclose that the client can initiate an FTP process to download files from a remote server, thereby showing that the client is capable of receiving data from said foreign network).

Consider **claim 3**, and **as it applies to claim 2 above**, Freund further discloses a system for the claimed invention, wherein said logic for monitoring operates to monitor data that said client receives from said foreign network (column 13, lines 60-64 which

disclose that if a process uses FTP to download a file, the system will match that activity to a file being saved by the same process by checking file name and size in order to invoke virus checking programs, thereby disclosing monitoring of data that the client downloaded from the remote FTP server).

Consider **claim 17**, and **as it applies to claim 1 above**, Freund further shows and discloses a system for the claimed invention, wherein said client is an employee workstation connected to an employer's local area network (Fig. 3A, client blocks 310a-c, column 14, lines 54-59, which disclose that the clients 310a-c may be personal computer or a workstation connected to a LAN 320).

Consider **claim 18**, and **as it applies to claim 2 above**, Freund further shows and discloses a system for the claimed invention, wherein said audit module and said audit database are part of said intermediary server (Fig. 3A, Supervisor block 323 embedded in proxy server 321; Fig. 5 that shows details of the supervisory functions including Data Interpretation Module 560 that includes audit module and Audit Log 580 and Exception Log 585 serving as an audit database; column 21, lines 41-46 which disclose that the functionality of an audit module is included within the data interpretation module 560, thereby disclosing that said audit module and said audit database are part of said intermediary server).

Consider **claim 19**, and **as it applies to claim 2 above**, Freund further shows and discloses a system for the claimed invention, wherein said audit module is part of said intermediary server (Fig. 3A, Supervisor block 323 embedded in proxy server 321; Fig. 5 that shows details of the supervisory functions including Data Interpretation Module 560 that includes audit module; column 21, lines 41-46 which disclose that the functionality of an audit module is included within the data interpretation module 560, thereby disclosing that said audit module is part of said intermediary server).

Consider **claim 20**, Freund shows and discloses a method for transparently auditing FTP traffic (Fig. 3A; column 4, lines 19-28 that disclose transparently auditing traffic; column 14, lines 52-67 and column 15, lines 1-11 that disclose the details of a method for monitoring network traffic; column 16, lines 25-29 that disclose monitoring of files transferred via FTP protocol) comprising:

defining a first computer to act as an intermediary between a second computer and a third computer (Fig. 3A, server block 321 as a first computer that acts as an intermediary between a second computer (client computers 310a-c) and a third computer (web server 350); column 14, lines 54-67 and column 15, lines 1-11 that disclose the same details);

defining an audit database (Fig. 5, audit log 580 used as an audit database; column 21, lines 41-46 that disclose the same details); and

defining an audit module (although Freund does not explicitly show a separate audit module, its functionality is incorporated within the data interpretation module 560

(shown in Fig. 5) that is part of the supervisory module 323 shown in Fig. 3A and disclosed in column 21, lines 41-46).

However, Freund does not explicitly define an audit module comprising logic for monitoring data transferred via an FTP protocol.

In the same field of endeavor, Peled et al. do show and disclose an audit module comprising logic for monitoring data transferred via FTP protocol (Fig. 1, Report Generator block 109 (same block listed as Audit Generator 409 in Fig. 4) along with the blocks 103, 105, and 106 that collectively provide logic for monitoring file transfer via FTP protocol; Fig. 9, FTP proxy block 980 with FTP Monitor 9801; paragraph 216, lines 5-10 that disclose an FTP proxy 980 in use).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include an audit module comprising logic for monitoring said data transferred via FTP protocol, as taught by Peled et al., in the method of Freund, so as to provide documented evidence of an employee's misuse of the company's IT resources.

Consider **claim 21**, and **as it applies to claim 20 above**, Freund further shows and discloses a method of the claimed invention, further comprising disposing said audit module in said first computer (column 21, lines 41-46 which disclose that the functionality of an audit module is included within the data interpretation module 560 (shown in Fig. 5) that is part of the supervisory module 323 shown in Fig. 3A).

Consider **claim 30**, Freund shows and discloses a mechanism for auditing data transferred via FTP (Fig. 3A; column 14, lines 52-67 and column 15, lines 1-11 that disclose a mechanism for auditing network traffic; column 16, lines 25-29 that disclose monitoring of files transferred via FTP protocol); comprising:

a means for transparently monitoring said data transferred via FTP (column 4, lines 19-28 that disclose transparently auditing traffic; column 16, lines 25-29 that disclose monitoring of files transferred via FTP protocol).

However, Freund does not explicitly disclose a means for recording at least a portion of said data transferred via an FTP protocol.

In the same field of endeavor, Peled et al. do show and disclose a means for recording at least a portion of said data transferred via an FTP protocol (Fig. 7, Audit Generator block 709; paragraph 0170, lines 13-21 that disclose recording relevant details of the transferred content stored in an audit database 110 shown in Fig. 1).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include a means for recording at least a portion of said data transferred via an FTP protocol, as taught by Peled et al., in the mechanism of Freund, so as to provide documented evidence of an employee's misuse of the company's IT resources.

Consider **claim 33**, Freund shows and discloses a system with computer programs for monitoring data transferred via an FTP protocol, the computer programs comprising code for transparently examining data transferred via an FTP protocol (Fig.

3A; column 4, lines 19-28 that disclose monitor programs transparently auditing network traffic; column 14, lines 52-67 and column 15, lines 1-11 that disclose the details of a method for monitoring network traffic; column 16, lines 25-29 that disclose monitoring of files transferred via FTP protocol).

However, Freund does not explicitly disclose code for recording at least a portion of said data transferred via an FTP protocol.

In the same field of endeavor, Peled et al. do show and disclose code for recording at least a portion of said data transferred via an FTP protocol (Fig. 7, Audit Generator block 709; paragraph 0170, lines 13-21 that disclose recording relevant details of the transferred content stored in an audit database 110 shown in Fig. 1).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include logic for recording at least a portion of said data transferred via FTP protocol to said audit database, as taught by Peled et al., in the computer program product of Freund, so as to provide documented evidence of an employee's misuse of the company's IT resources.

Consider **claim 34**, and **as it applies to claim 33 above**, Freund discloses a system with computer programs for the claimed invention, except wherein said code for transparently examining comprises code for determining an origination point of said data transferred via an FTP protocol and code for determining an end point of said data transferred via an FTP protocol.

In the same field of endeavor, Peled et al. disclose a system with computer programs for determining an origination point of said data transferred via an FTP protocol and code for determining an end point of said data transferred via an FTP protocol (paragraph 0170, lines 13-21 which disclose that both the source (origination point) and the destination (end point) of the FTP data transfer are being recorded, thereby disclosing presence of code for determining an origination point of said data transferred via an FTP protocol and code for determining an end point of said data transferred via an FTP protocol).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include code for determining an origination point of said data transferred via an FTP protocol and code for determining an end point of said data transferred via an FTP protocol, as taught by Peled et al., in the system with computer programs of Freund, so as to provide complete details in a documented evidence showing an employee's misuse of the company's IT resources.

Consider **claim 35**, and **as it applies to claim 34 above**, Freund discloses a system with computer programs for the claimed invention, including code for determining a filesize of said data transferred via an FTP protocol (column 13, lines 60-64 that disclose saving the size of the received file).

However, Freund does not disclose that said code for transparently examining further comprises code for determining a filename of said data transferred via an FTP

protocol and code for determining a date said data transferred via an FTP protocol was transferred.

In the same field of endeavor, Peled et al. disclose a system with computer programs for determining a filename of said data transferred via an FTP protocol and code for determining a date said data transferred via an FTP protocol was transferred (paragraph 0170, lines 13-21 that disclose content name (filename) and time (date) of the FTP data transfer being recorded).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include code for determining a filename of said data transferred via an FTP protocol and code for determining a date said data transferred via an FTP protocol was transferred, as taught by Peled et al., in the system with computer programs of Freund, so as to provide complete details in a documented evidence showing an employee's misuse of the company's IT resources.

Claims 5, 22 and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Freund (U.S. Patent Publication # 5,987,611)** in view of **Peled et al. (U.S. Patent Application Publication # 2002/0129140 A1)** and further in view of **Trcka et al. (U.S. Patent Publication # 6,453,345 B2).**

Consider **claim 5**, and **as it applies to claim 3 above**, Freund, as modified by Peled et al., discloses a system for the claimed invention, except wherein said logic for recording operates to record all data that said client receives from said foreign network.

In the same field of endeavor, Trcka et al. show and disclose a system wherein said logic for recording operates to record all data that said client receives from said foreign network (Fig. 3, Archival Data Processing Module 90, Archival Media unit 80, that record every packet received or sent from the LAN network; column 2, lines 15-33 that disclose the same details).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include logic in the audit module for recording at least a portion of data transferred via FTP protocol operates to record all data that said client receives from said foreign network, as taught by Trcka et al., in the system of Freund, as modified by Peled et al., so as to provide means for recovering lost file data or damaged or corrupted packets.

Consider **claim 22**, and **as it applies to claim 20 above**, Freund, as modified by Peled et al., discloses a method for the claimed invention, except recording said data transferred via an FTP protocol to said audit database.

In the same field of endeavor, Trcka et al. show and disclose a method for recording said data transferred via an FTP protocol to said audit database (Fig. 3, Archival Data Processing Module 90, Archival Media unit 80, that record every packet received or sent from the LAN network; column 2, lines 15-33 and 56-61 which disclose that the archived data may be used for auditing functions).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include recording said data transferred via an FTP

protocol to said audit database, as taught by Trcka et al., in the method of Freund, as modified by Peled et al., so as to provide means for performing low level analyses of network break-ins and other auditing functions.

Consider **claim 24**, and **as it applies to claim 20 above**, Freund, as modified by Peled et al., discloses a method for the claimed invention, including wherein said logic for monitoring data transferred via an FTP protocol comprises:
monitoring an FTP control port of a computer receiving said data transferred via an FTP protocol and monitoring an FTP data port of said computer receiving said data transferred via an FTP protocol (In Peled et al. reference, paragraph 0205, lines 17-25 that disclose monitoring Data and Control ports during an FTP file transfer).

However, Freund, as modified by Peled et al., does not disclose a method for recording said data transferred via an FTP protocol to said audit database when said logic for monitoring said FTP data port determines that a request to transfer data via said FTP data port has occurred.

In the same field of endeavor, Trcka et al. show and disclose a method for recording said data transferred via an FTP protocol to said audit database (Fig. 3, Archival Data Processing Module 90, Archival Media unit 80, that record every packet received or sent from the LAN network; column 2, lines 15-33 and 56-61 which disclose that the archived data may be used for auditing functions).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include recording said data transferred via an FTP

protocol to said audit database, as taught by Trcka et al., in the method of Freund, as modified by Peled et al., so as to provide complete details in a documented evidence showing an employee's misuse of the company's IT resources.

Consider **claim 25**, and **as it applies to claim 22 above**, Freund as modified by Peled et al. and Trcka et al., further shows and discloses a method of the claimed invention, wherein said second computer is located in a intranet and said third computer is located in a network that is foreign to said intranet (In Freund reference, Fig. 3A, that shows client computers (second computer) on a LAN (Intranet); and Web Servers (third computer) 350 as remote computers with the Internet in between; column 14, lines 54-67 and column 15, lines 1-11 that disclose the same details).

Consider **claim 26**, and **as it applies to claim 25 above**, Freund as modified by Peled et al. and Trcka et al. further shows and discloses a method, wherein said data transferred via an FTP protocol is recorded to said audit database upon a finding of either one of said second computer connecting to said third computer and said second computer sending data from said second computer to said third computer; and said second computer connecting to said third computer and said second computer receiving data sent from said third computer to said second computer (Fig. 3, Archival Data Processing Module 90, Archival Media unit 80, that record every packet received or sent from the LAN network; column 2, lines 15-33 that disclose the same details).

Claims 6, 9, 10, 31 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Freund (U.S. Patent Publication # 5,987,611)** in view of **Peled et al. (U.S. Patent Application Publication # 2002/0129140 A1)**, and further in view of **Touboul et al. (U.S. Patent Application Publication # 2004/0153515 A1).**

Consider **claim 6**, and **as it applies to claim 3 above**, Freund, as modified by Peled et al., discloses a system for the claimed invention, except wherein said audit module further comprises logic for recording metadata associated with said data that said client receives from said foreign network.

In the same field of endeavor, Touboul et al. show and disclose a system wherein said audit module further comprises logic for recording metadata associated with said data that said client receives from said foreign network (Fig. 1, Auditor block 172; paragraph 0049, that disclose the document type metadata, such as creation date, author's name, etc. being recorded in an audit record).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include logic in the audit module for recording metadata associated with said data that said client receives from said foreign network, as taught by Touboul et al., in the system of Freund, as modified by Peled et al., so as to provide complete details in a documented evidence showing an employee's misuse of the company's IT resources.

Consider **claim 9**, and **as it applies to claim 1 above**, Freund, as modified by Peled et al., discloses a system for the claimed invention, except wherein said client is capable of transferring data to said foreign network.

In the same field of endeavor, Touboul et al. show and disclose a system wherein said client is capable of transferring data to said foreign network (Fig. 1, clients 130 showing bi-directional communication arrows to the Internal Traffic Monitor 113 and bi-directional external traffic arrows to the External Traffic Monitor 117, thereby showing both inbound and outbound traffic capability for the clients 130; paragraph 0048, lines 6-9 that define a transaction as a transmission of a designated document sent from a source to a destination, or received by a source from a destination; destination being shown as internal or external in Fig. 1).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide capability to said client of transferring data to said foreign network, as taught by Touboul et al., in the system of Freund, as modified by Peled et al., so as to provide an employee proper means for conducting authorized company business with external customers.

Consider **claim 10**, and **as it applies to claim 9 above**, Freund, as modified by Peled et al. and Touboul et al., further discloses a system wherein said logic for monitoring operates to monitor data that said client transfers to said foreign network (Fig. 1, Internal Traffic Monitor block 113 and External Traffic Monitor block 117 along with Monitoring Engine 120 that monitor and analyze both inbound and outbound network traffic; paragraph 0048 that discloses the details of the Monitoring Engine 120).

Consider **claim 31**, and **as it applies to claim 30 above**, Freund as modified by Peled et al., discloses a mechanism of the claimed invention, except further disclosing comprising a means for recording metadata associated with said data transferred via FTP.

In the same field of endeavor, Touboul et al. show and disclose a mechanism further comprising a means for recording metadata associated with said data transferred via FTP (Fig. 1, Auditor block 172; paragraph 0049, that disclose the document type metadata, such as creation date, author's name, etc. being recorded).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to means for recording metadata associated with said data transferred via FTP, as taught by Touboul et al., in the mechanism of Freund, as modified by Peled et al., so as to provide complete details in a documented evidence showing an employee's misuse of the company's IT resources.

Consider **claim 32**, and **as it applies to claim 31 above**, Freund as modified by Peled et al., discloses a mechanism of the claimed invention, except wherein said means for recording further comprises a means for organizing said data transferred via FTP.

In the same field of endeavor, Touboul et al. disclose a means for recording further comprises a means for organizing said data transferred via FTP (metadata fields

for document ID, sender, recipients, and date in paragraphs 0061-0064); these fields being stored in the audit record (paragraph 0059) which is a table based structure.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to organize metadata fields for said data transferred via FTP, as taught by Touboul et al., in the mechanism of Freund, as modified by Peled et al.,so as to provide easy retrieval of any selected field from the database using SQL type queries.

Claims 4, 7, 8, 11-16, 23, 27-29, 36-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Freund (U.S. Patent Publication # 5,987,611)** in view of **Peled et al. (U.S. Patent Application Publication # 2002/0129140 A1)**, and further in view of **Touboul et al. (U.S. Patent Application Publication # 2004/0153515 A1),** and further in view of **Trcka et al. (U.S. Patent Publication # 6,453,345 B2).**

Consider **claim 4**, and **as it applies to claim 3 above**, Freund, as modified by Peled et al., discloses a system for the claimed invention, except wherein said audit module further comprises logic for recording metadata associated with said data that said client receives from said foreign network; and wherein said logic for recording at least a portion of data transferred via FTP protocol operates to record all data that said client receives from said foreign network.

In the same field of endeavor, Touboul et al. show and disclose a system wherein said audit module further comprises logic for recording metadata associated with said data that said client receives from said foreign network (Fig. 1, Auditor block

172; paragraph 0049, that disclose the document type metadata, such as creation date, author's name, etc. being recorded in an audit record).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include logic in the audit module for recording metadata associated with said data that said client receives from said foreign network, as taught by Touboul et al., in the system of Freund, as modified by Peled et al., so as to provide complete details in a documented evidence showing an employee's misuse of the company's IT resources.

However, Freund as modified by Peled et al. and Touboul et al., does not explicitly disclose that said logic for recording at least a portion of data transferred via FTP protocol operates to record all data that said client receives from said foreign network.

In the same field of endeavor, Trcka et al. show and disclose a system wherein said logic for recording at least a portion of data transferred via FTP protocol operates to record all data that said client receives from said foreign network (Fig. 3, Archival Data Processing Module 90, Archival Media unit 80, that record every packet received or sent from the LAN network; column 2, lines 15-33 that disclose the same details).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include logic in the audit module for recording at least a portion of data transferred via FTP protocol operates to record all data that said client receives from said foreign network, as taught by Trcka et al., in the system of

Freund, as modified by Peled et al. and Touboul et al., so as to provide means for recovering lost file data or damaged or corrupted packets.

Consider **claim 7**, and **as it applies to claim 4 above**, Freund, as modified by Peled et al., Touboul et al. and Trcka et al., further discloses a system for the claimed invention, wherein said logic for recording all data operates to record said data only if said logic for monitoring said data transferred via FTP protocol determines that said data that said client receives from said foreign network comprises at least one of pornographic data, image data, audio data, and terrorist activity data (In Freund reference column 24, lines 7-9 that disclose an administrator blocking user access to pornographic sites).

Consider **claim 8**, and **as it applies to claim 5 above**, Freund, as modified by Peled et al. and Trcka et al., discloses a system for the claimed invention, except wherein said audit module further comprises company guidelines defining acceptable content wherein said logic for recording all data operates to record said data only if said audit module determines that said data that said client receives from said foreign network is in violation of said company guidelines.

In the same field of endeavor, Touboul et al. show and disclose a system wherein said audit module further comprises company guidelines defining acceptable content wherein said logic for recording all data operates to record said data only if said audit module determines that said data that said client receives from said foreign

network is in violation of said company guidelines (Fig. 2, flowchart blocks 235, 240, 245, 225 and 230 that disclose a company policy to either allow or disallow transmission of documents from a sender to certain receivers and generate audit record and log event; paragraphs 0055-0057 that disclose the same details).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include logic in the audit module for company guidelines defining acceptable content wherein said logic for recording all data operates to record said data only if said audit module determines that said data that said client receives from said foreign network is in violation of said company guidelines, as taught by Touboul et al., in the system of Freund, as modified by Peled et al. and Trcka et al., so as to impress upon the employees that misuse the company's IT resources, the consequences of their actions.

Consider **claim 11**, and **as it applies to claim 9 above**, Freund, as modified by Peled et al., Touboul et al., discloses a system for the claimed invention, except wherein said logic for recording data operates to record all data that said client transfers to said foreign network.

In the same field of endeavor, Trcka et al. show and disclose a system wherein said logic for recording data operates to record all data that said client transfers to said foreign network (Fig. 3, Archival Data Processing Module 90, Archival Media unit 80, that record every packet received or sent from the LAN network; column 2, lines 15-33 that disclose the same details).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include logic in the audit module for recording data operates to record all data that said client transfers to said foreign network, as taught by Trcka et al., in the system of Freund, as modified by Peled et al. and Touboul et al., so as to provide means for recovering lost file data or damaged or corrupted packets.

Consider **claim 12**, and **as it applies to claim 11 above**, Freund, as modified by Peled et al., Touboul et al. and Trcka et al., further discloses a system for the claimed invention, wherein said audit module further comprises logic for recording metadata associated with said data that said client transfers to said foreign network (In Touboul et al. reference, Fig. 1, Auditor block 172; paragraph 0049, that disclose the document type metadata, such as creation date, author's name, etc. being recorded in an audit record).

Consider **claim 13**, and **as it applies to claim 10 above**, Freund, as modified by Peled et al., Touboul et al. and Trcka et al., further discloses a system for the claimed invention, wherein said audit module further comprises logic for recording metadata associated with said data that said client transfers to said foreign network (In Touboul et al. reference, Fig. 1, Auditor block 172; paragraph 0049, that disclose the document type metadata, such as creation date, author's name, etc. being recorded in an audit record); and

wherein said logic for recording at least a portion operates to record all data that said client transfers to said foreign network (In Trcka et al. reference, Fig. 3, Archival Data Processing Module 90, Archival Media unit 80, that record every packet received or sent from the LAN network; column 2, lines 15-33 that disclose the same details).

Consider **claim 14**, and **as it applies to claim 13 above**, Freund, as modified by Peled et al., Touboul et al. and Trcka et al., further discloses a system for the claimed invention, wherein said logic for recording all data that said client transfers to said foreign network operates to record said data only if said logic for monitoring said data transferred via FTP protocol determines that said data that said client transferred to said foreign network comprises at least one of proprietary company information; confidential company information; pornographic data; image data; audio data; and terrorist activity data (In Touboul et al. reference, paragraph 0054, lines 4-18 that disclose blocking the transmission of company confidential data to outside recipients and recording the event in an audit log).

Consider **claim 15**, and **as it applies to claim 11 above**, Freund, as modified by Peled et al., Touboul et al. and Trcka et al., further discloses a system for the claimed invention, wherein said audit module further comprises company guidelines defining acceptable content wherein said logic for recording all data that said client transfers to said foreign network operates to record said data only if said audit module determines that said data that said client transferred to said foreign network is in violation of said

company guidelines (In Touboul et al. reference, Fig. 2, flowchart blocks 235, 240, 245, 225 and 230 that disclose a company policy to either allow or disallow transmission of documents from a sender to certain receivers and generate audit record and log event; paragraph 0048 that disclose the same details).

Consider **claim 16**, and **as it applies to claim 1 above**, Freund as modified by Peled et al. discloses a system for the claimed invention, including saving in an audit record a field to store data related to a size of said transferred data (In Freund reference, column 13, lines 60-64 that disclose saving the size of the received file in an audit log record);

However, Freund as modified by Peled et al., does not explicitly disclose a table structure for said audit database organized to comprise a field to store data related to a client who originated a transfer of said data; a field to store data related to a destination of said transferred data; a field to store data related to a name of said transferred data; and a field to store data related to a date that said data was transferred; and a field to store said transferred data.

In the same field of endeavor, Touboul et al. disclose a table structure for said database (paragraph 0058, lines 9-10 that disclose a table structure for an audit record) organized to comprise:

a field to store data related to a client who originated a transfer of said data (paragraph 0062);

a field to store data related to a destination of said transferred data (paragraph 0063);

a field to store data related to a name of said transferred data (paragraph 0061); and a field to store data related to a date that said data was transferred (paragraph 0064).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include a field to store data related to a client who originated a transfer of said data; a field to store data related to a destination of said transferred data; a field to store data related to a name of said transferred data; and a field to store data related to a date that said data was transferred, as taught by Touboul et al., in the system of Freund as modified by Peled et l., so as to provide complete details for a documented evidence of an employee's misuse of the company's IT resources.

However, Freund as modified by Peled et al. and Touboul et al., does not explicitly disclose a table structure for said database organized to comprise a field to store said transfer data.

In the same field of endeavor, Trcka et al. disclose storing said transferred data (Fig. 3, Archival Data Processing Module 90, Archival Media unit 80, that record every packet received or sent from the LAN network; column 2, lines 15-33 that disclose the same details).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to store said transferred data, as taught by Trcka et al., in the system of Freund as modified by Peled et l. and Touboul et al., so as to provide complete details for a documented evidence of an employee's misuse of the company's IT resources.

Consider **claim 23**, and **as it applies to claim 22 above**, Freund, as modified by Peled et al. and Trcka et al., discloses a method of the claimed invention, except recording metadata associated with said data transferred via an FTP protocol to said audit database.

In the same field of endeavor, Touboul et al. disclose a method comprising recording metadata associated with said data transferred via an FTP protocol to said audit database (Fig. 1, Auditor block 172; paragraph 0049, that disclose the document type metadata, such as creation date, author's name, etc. being recorded in an audit record).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to record metadata associated with said data transferred via an FTP protocol to said audit database, as taught by Touboul et al., in the method of Freund, as modified by Peled et al., so as to provide complete details in a documented evidence showing an employee's misuse of the company's IT resources.

Consider **claim 27**, and **as it applies to claim 26 above**, Freund, as modified by Peled et al. and Trcka et al., discloses a method of the claimed invention, including monitoring for FTP file transfer from pornographic sites (In Freund reference, column 24, lines 7-9 that disclose pornographic data being monitored).

However, Freund, as modified by Peled et al. and Trcka et al., does not explicitly disclose a method of selectively recording said data received from said third computer only upon a finding by said logic for monitoring data transferred via an FTP protocol that

said received data comprises at least one of: pornographic data; image data; audio data; and terrorist activity data.

In the same field of endeavor, Touboul et al. disclose a method of selectively recording said data received from said third computer only upon a finding by said logic for monitoring data transferred via an FTP protocol (In Touboul et al. reference, Fig. 2, flowchart blocks 235, 240, 245, 225 and 230 that disclose a company policy to either allow or disallow transmission of documents from a sender to certain receivers and generate audit record and log event; paragraph 0048 that disclose the same details).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to selectively record said data received from said third computer only upon a finding by said logic for monitoring data transferred via an FTP protocol that said received data comprises at least one of: pornographic data; image data; audio data; and terrorist activity data, as taught by Touboul et al., in the method of Freund as modified by Peled et l. and Trcka et al., so as to provide complete details for a documented evidence of an employee's misuse of the company's IT resources.

Consider **claim 28**, and **as it applies to claim 26 above**, Freund, as modified by Peled et al., Touboul et al., and Trcka et al., further discloses a method of the claimed invention, defining company guidelines that define acceptable content wherein said data received from said third computer will be recorded only upon a finding by said logic for monitoring data transferred via an FTP protocol that said received data is in violation of said company guidelines (In Freund reference, column 23, lines 65-67 and column 24, lines 1-15 that disclose an administrator setting company's guidelines and rules for

acceptable content; and in Touboul reference, Fig. 2, flowchart blocks 235, 240, 245, 225 and 230 that disclose a company policy to either allow or disallow transmission of documents from a sender to certain receivers and generate audit record and log event; paragraph 0048 that disclose the same details).

Consider **claim 29**, and **as it applies to claim 26 above**, Freund, as modified by Peled et al. and Trcka et al., discloses a method of the claimed invention, except wherein said data sent from said second computer to said third computer will be recorded only upon a finding by said logic for monitoring data transferred via an FTP protocol that said transferred data comprises at least one of: proprietary company information; confidential company information; pornographic data; image data; audio data; and terrorist activity data.

In the same field of endeavor, Touboul et al. disclose a method of the claimed invention, wherein said data sent from said second computer to said third computer will be recorded only upon a finding by said logic for monitoring data transferred via an FTP protocol that said transferred data comprises at least one of: proprietary company information; confidential company information; pornographic data; image data; audio data; and terrorist activity data (In Touboul et al. reference, paragraph 0054, lines 4-18 that disclose blocking the transmission of company confidential data to outside recipients and recording the event in an audit log).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to selectively record said data sent from said second computer to said third computer only upon a finding by said logic for monitoring data

transferred via an FTP protocol that said transferred data comprises at least one of: proprietary company information; confidential company information; pornographic data; image data; audio data; and terrorist activity data, as taught by Touboul et al., in the method of Freund as modified by Peled et l. and Trcka et al., so as to provide complete details for a documented evidence of an employee's misuse of the company's IT resources.

Consider **claim 36**, and **as it applies to claim 34 above**, Freund, as modified by Peled et al., discloses a system with computer code for the claimed invention, except wherein said code for recording comprises code for recording said data transferred via an FTP protocol; and code for recording metadata associated with said data transferred via an FTP protocol.

In the same field of endeavor, Touboul et al. show and disclose a system with computer code for recording metadata associated with said data transferred via an FTP protocol (Fig. 1, Auditor block 172; paragraph 0049, that disclose the document type metadata, such as creation date, author's name, etc. being recorded in an audit record).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide a system with computer code for recording metadata associated with said data transferred via an FTP protocol, as taught by Touboul et al., in the system with programming code of Freund, as modified by Peled et al., so as to provide complete details in a documented evidence showing an employee's misuse of the company's IT resources.

However, Freund as modified by Peled et al. and Touboul et al., does not explicitly disclose that said code for recording comprises code for recording said data transferred via an FTP protocol.

In the same field of endeavor, Trcka et al. show and disclose a system with programming code for recording said data transferred via an FTP protocol (Fig. 3, Archival Data Processing Module 90, Archival Media unit 80, that record every packet received or sent from the LAN network; column 2, lines 15-33 that disclose the same details).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to include code for recording said data transferred via an FTP protocol, as taught by Trcka et al., in the system with programming code of Freund, as modified by Peled et al. and Touboul et al., so as to provide means for recovering lost file data or damaged or corrupted packets, as well as for archiving and auditing purposes.

Consider **claim 37**, and **as it applies to claim 36 above**, Freund as modified by Peled et al., Touboul et al. and Trcka et al., further discloses a system with computer programs for the claimed invention, wherein said code for transparently examining data further comprises code for determining if said data transferred via an FTP protocol is suspicious wherein said data transferred via an FTP protocol is suspicious if said data transferred via an FTP protocol comprises at least one of proprietary company information; confidential company information, pornographic data; image data; audio

data; and terrorist activity data (In Touboul et al. reference, paragraph 0054, lines 4-18 that disclose blocking the transmission of company confidential data to outside recipients and recording the event in an audit log, thereby disclosing presence of code to monitor suspicious data).

Consider **claim 38**, and **as it applies to claim 36 above**, Freund as modified by Peled et al., Touboul et al. and Trcka et al., further discloses a system with computer programs for the claimed invention, wherein said code for transparently examining further comprises:

code defining company guidelines that define acceptable content (column 23, lines 66-67 and column 24, lines 1-15 that disclose programming code providing company guidelines that define acceptable content); and

code for determining if said data transferred via an FTP protocol is in violation of said company guidelines (In Touboul et al reference, paragraph 0054, lines 4-18 that disclose blocking the transmission of company confidential data to outside recipients and recording the event in an audit log, thereby disclosing presence of code to determine if said data transferred via an FTP protocol is in violation of said company guidelines).

Consider **claim 39**, and **as it applies to claim 38 above**, Freund as modified by Peled et al., Touboul et al. and Trcka et al., further discloses a system with computer programs for the claimed invention, wherein said code for recording data transferred via an FTP protocol executes to record said data transferred via an FTP protocol only if

said code for transparently examining determines that said data transferred via an FTP protocol is in violation of company guidelines (In Touboul et al reference, paragraph 0054, lines 4-18 that disclose blocking the transmission of company confidential data to outside recipients and recording the event in an audit log, thereby disclosing presence of code to determine if said data transferred via an FTP protocol is in violation of said company guidelines, then recording said data in a log event).

Consider **claim 40**, and **as it applies to claim 37 above**, Freund as modified by Peled et al., Touboul et al. and Trcka et al., further discloses a system with computer programs for the claimed invention, wherein said code for recording said data transferred via an FTP protocol will record said data transferred via an FTP protocol only if said data transferred via an FTP protocol is suspicious (In Touboul et al reference, paragraph 0054, lines 4-18 that disclose blocking the transmission of company confidential data to outside recipients and recording the event in an audit log, thereby disclosing presence of code to determine if said data transferred via an FTP protocol is suspicious, then recording said data in an audit log).

Conclusion

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Kishin G. Belani whose telephone number is (571) 270-1768. The Examiner can normally be reached on Monday-Thursday from 6:30 am to 5:00 pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, David Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-0800.

Kishin G. Belani

K.G.B./kgb

August 5, 2007

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100